Software & Information
Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4095

Comments of the

SOFTWARE & INFORMATION INDUSTRY ASSOCIATION

to the U.S. Department of Commerce Internet Policy Task force on

COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK

January 28, 2010

On behalf of the members of the Software & Information Industry Association (SIIA), we appreciate the opportunity to respond to the green paper entitled "*Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework,"* (Report) released on December 21, 2010, requesting public comment on the impact of the current privacy laws in the United States and around the world on the pace of innovation in the information economy.

As the principal trade association of the software and digital information industry, the more than 500 members of SIIA develop and market software and electronic content for business, education and consumers.[1] SIIA's members are software companies, e-businesses, and information service companies, as well as many electronic commerce companies. As leaders in the global market for software and information products and services, our membership consists of some of the largest and oldest technology enterprises in the world, as well as many smaller and newer companies.

For over a decade, SIIA has worked with policymakers at the Federal and state levels in the United States, and also with policymakers in Europe, Canada and other regions, to examine the implications and operations of privacy and related laws. This has included work with the relevant Federal agencies implementing existing privacy and security regulations and policies, notably, the Federal Trade Commission's (FTC) approach on unfair trade practices, as well as implementation of Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and the Health IT Act, as well as state policy makers considering myriad state laws on privacy and data security, and foreign governments, notably Canada and the European Union (EU).

[1] Our website can be found at: www.siia.net

Tel: +1.202.289.7442
Fax: +1.202.289.7097
www.siia.net

GENERAL COMMENTS

As we noted in our comments in response to the Notice of Inquiry (NOI) issued in April 2010, we greatly appreciate the thorough consideration being given to this important issue by the Department of Commerce (Department) Internet Policy Task Force (Task Force), and the opportunity to provide input.

In general SIIA supports most of the recommendations in the Report. Particularly, SIIA supports the following key tenets:

- **SIIA strongly supports the emphasis on the balance between privacy and the free flow of information, as well as the balance between the need for consumer confidence and continued innovation to propel e-commerce to continue fueling U.S. economic growth**. Indeed, as the Report identifies, given the critical nature of consumer confidence, commercial data privacy protection is critical to ensuring that the Internet fulfills its social and economic potential.

  The Internet economy today far surpasses Vice President Gore's prediction, with the economic benefits of the commercial Internet eclipsing the global sales of medicine, investment in renewable energy, and government investment in R&D, combined.[2] "And if e-commerce continues to grow annually *half as fast* as it grew between 2005 and 2010, then by 2020 global e-commerce will reach $24.2 trillion, and will add roughly $3.8 trillion annually to the global economy – more than the total GDP of Germany."[3]

  As the convergence of software and information (S&I) have combined to transform the way that users—individual consumers, government, business end users, and enterprises—access news and information, deliver products and services, and operate, the S&I industries have become strong drivers of the U.S. and global economies, and they are also driving the digital revolution across virtually all sectors of the economy. Well-known firms as well as new, emerging startups—many of which are members of SIIA—create transformative products and services at the leading edge of innovation.

  By any measure, the substantial economic impact of the S&I industries demonstrates the critical role that these industries play in a vibrant and dynamic U.S. and global economy.[4] The S&I industries have been over the last decade and remain today among the fastest growing and most important for creating jobs and propelling continued U.S. economic growth. For instance, in 2005, S&I industry growth was up nearly 11 percent, compared with 3.2 percent for the economy as a whole, while software and information generated $564 billion in revenue.

---

[2] Atkinson, et al, *The Internet Economy 25 Years After .com: Transforming Commerce & Life*, Information Technology & Innovation Foundation, March 2010, pg. 43, available at:

[3] Ibid (emphasis added).

[4] *Software and Information: Driving the Global Knowledge Economy,* SIIA, January 2008, pg. 11, available at: http://www.siia.net/estore/globecon-08.pdf.

Of course, this growth and innovation would not be possible without a policy framework that strikes the right balance between privacy with the free flow of information. As initiated during the Clinton Administration's Framework for Global Electronic Commerce and reiterated in this Report, it is essential that the U.S. continue to maintain this critical balance.

- **SIIA commends the Task Force for relying heavily on input and leadership from the private sector, for encouraging an industry self-regulation framework, rather than Government regulation, and for stressing the need for a "cooperative, multi-stakeholder approach."** It is greatly beneficial, as suggested in the Report, that the Government's role be primarily as a coordinator in this process, acting as a convener of the many stakeholders that share the interest of continued development of the digital marketplace. As highlighted by the Report, this is the role that was established in the 1990s as the commercial Internet was emerging. Indeed, this is a core approach that should never be overlooked with respect to the digital marketplace. As proposed by the report, voluntary, enforceable codes of conduct are the appropriate approach for privacy protections because they develop faster and provide more flexibility than legislation or regulation.

- **SIIA agrees that for many reasons, the Department of Commerce is well served to lead the Administration's efforts to explore policy in this area.** First, the Task Force, created by Secretary Locke to bring together the technical, policy, trade and legal expertise of the Department is well equipped to lead this effort. Indeed, the Task Force is front-and-center in this effort through its leadership role in examining policy approaches that reduce barriers to digital commerce while advocating for adequate protections for commercial data privacy, cybersecurity, intellectual property and the global free flow of information. Further, as highlighted in the Report, the Department's leadership is based-upon the National Telecommunications and Information Administration (NTIA), as a principal adviser to the President on telecommunications and information policies, the International Trade Administration (ITA) as a proponent of policy frameworks to facilitate the free flow of data across borders, as well as the growth of digital commerce and international trade, and the National Institute of Standards and Technology (NIST) as a leader in the area of encouraging the development of key technology standards.

  In addition to this leadership in expertise and a proven ability to engage in the inter-agency process, the Department also plays a critical role as a proponent of U.S. businesses worldwide, effectively leading in this debate with our major international trading partners. Indeed, led by the Department, the U.S. is in a strong position to demonstrate in global conversations that a voluntary, self-regulation framework provides strong privacy protections.

- **SIIA strongly agrees that the Internet has thrived for decades now, largely as a result of the fact that U.S. Internet policy has avoided fragmented, prescriptive, and unpredictable rules that frustrate innovation and undermine consumer trust in this arena**. This has always been a shared objective of both industry and policymakers alike. The United States has developed a model that facilitates transparency, promotes cooperation, and strengthens multi-stakeholder governance that has allowed innovation to flourish while building trust and protecting a broad array of other rights and interests. And we therefore concur that "we must proceed in a way that fully recognizes the digital economy's complexity and dynamism."

- **SIIA appreciates the Department's approach to avoid recommending a policy at this time, but rather, to recognize that the Report is just the beginning of the policy discussions within the Obama Administration**. Given the complexity of this issue and the importance of the multi-stakeholder approach, combined with the fact that the Internet continues to evolve rapidly, hasty recommendations are not helpful in this environment. We commend the Department and, more broadly the Administration, for taking a thorough, thoughtful approach.

SIIA COMMENTS ON PROPOSED POLICY OPTIONS FOR A DYNAMIC POLICY FRAMEWORK FOR COMMERCIAL DATA

Bolstering Consumer Trust Online Through 21st Century Fair Information Practice Principles

As a general matter, SIIA concurs with the objective to achieve increased transparency through simple notices, clearly articulated purposes for data collection, commitments to limit data uses to fulfill these purposes and expanded use of robust audit systems to bolster accountability. A Fair Information Practice Principles (FIPPs) approach is useful for companies to analyze their practices, and it could be an effective foundation for commercial data privacy. If applied correctly, such an approach could help to achieve the stated goal of promoting informed consent without imposing undue burdens on commerce and on commercial actors.

However, we are concerned that this approach would not be effective as a legislated or mandatory regulatory framework. A significant number of companies do not collect data directly from consumers, making it difficult to provide notice or to obtain consent. Other companies work with individuals in their capacity as representatives of businesses, not in their personal capacity as consumers, and the same protections should not apply to business contact data. There should be a business contact information exception that allows the use of business contact information of the type that appears on business cards or letterhead without notice and consent, perhaps on the theory that consent has been given implicitly as part of the decision to make such

information available. It is not practical to apply FIPPs to all data practices, as not all types or uses of data should be subject to a FIPPs framework.

Advancing Consumer Privacy Through a focus on Transparency, Purpose Specification, Use Limitation, and Auditing

SIIA agrees that transparency plays a key role in moving the U.S. privacy policy framework forward, but we would also point out that it is a delicate balance between providing policies that are succinct and easily understood by all consumers and those that are legally sufficient. Unfortunately, the objectives of reduced length and greater simplicity in privacy policies are sometimes inconsistent with the objective of ensuring well-informed choice by consumers and legal adequacy to protect the interests of the business.

SIIA agrees that technology can play a key role in bringing about greater transparency to privacy practices. To that end, companies continue to develop preference management tools to allow customers to express their preferences with respect to the types of advertising they receive. These technological advancements are a great example of how industry self-regulation has enabled companies to develop transparency mechanisms that adequately meet the needs of their consumers while also fitting their business models.

Maintaining Dynamic Privacy Protections Through Voluntary, Enforceable, FTC-Approved Codes of Conduct

SIIA concurs that commercial data privacy policy must be able to evolve rapidly to meet a continuing stream of innovations. Further we are very supportive of the Department's approach to enlist the expertise and knowledge of the private sector and to rely on industry best practices in an effort to create voluntary codes of conduct that promote informed consent and safeguard personal information. Most likely, the Government, led by the Department of Commerce, could have the greatest contribution to this effort in helping to encourage stakeholders to develop and implement such voluntary codes of conduct, rather than as a regulator. With respect to the proposal to establish a Privacy Policy Office within the Department, initial considerations reveal that this would quite likely have the affect of duplicating ongoing efforts.

SIIA is concerned that the implementation of privacy principles through legislation or rulemaking would not be effective, and may even be counterproductive. Further, we do not believe that it is necessary to expand the FTC's enforcement power beyond its current authority or provide a private right of action to consumers. The FTC already has wide enforcement power of consumer privacy protection under numerous sector-specific statutes and Section 5 of the FTC Act. As discussed in the FTC's *Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A*

Proposed Framework for Businesses and Policymakers, the FTC has capably used its authority under these statutes to bring cases against businesses that allegedly failed to protect consumers' personal information. In the last ten years alone, the FTC has brought 29 such cases. The FTC has also brought over one hundred cases involving unwanted spam, spyware, and violations of the Childrens' Online Privacy Protection Act (COPPA).

To police those entities that commit to follow voluntary codes of conduct, we recommend the use of industry accountability programs, similar to those developed by the Direct Marketing Association (DMA), the National Advertising Review Council and its administrator, the Council of Better Business Bureaus. These programs have a long history of successfully ensuring compliance and accountability as well as cooperation with the FTC, and this approach is consistent with the Department's desire to utilize industry best practices in an effort to create voluntary codes of conduct.

Encourage Global Interoperability

As discussed above, technology innovation and the Internet economy remain the engine of growth for the U.S. economy, producing high wage and high value jobs in an increasingly globally competitive marketplace. Cross-border flows of consumer and user data are essential to preserving the competitiveness of U.S. workers and U.S. enterprises, and the Department should work to ensure that data protection laws do not impose barriers to trade.

Currently, a variety of domestic and foreign laws govern how companies collect, use and share data about individuals. In addition, an increasing array of domestic and foreign laws address the security, retention and even accuracy of such information. This web of laws affects individuals in a variety of contexts: as individual consumers, as employees, and as persons doing business publicly.

This is occurring as U.S. enterprises that are at the heart of the digital and Internet economy increasingly look outward from their U.S. bases to find new customers, enter new markets, and reap the benefits of delivering online services and products without having the costs of traditional 'brick-and-mortar' localization imposed, which may mitigate the opportunity risks.[5] This is true not just for larger enterprises, but also for

[5] The Task Force should recall that central to Free Trade Agreements negotiated by the US, starting with Chile and Singapore, is a strategic definition of "digital product" that is not inherently tied to either a goods or services trade law framework and does not prejudice a product's classification. By broadly defining "digital product" to include computer programs, text, video, images, sound recordings and other products that are digitally encoded, regardless of whether they are fixed on a carrier medium or transmitted electronically, the FTAs seek a flexible, but practical approach to ensuring that goods and services that combine elements of any of these items are not discriminated against. In other words, no matter how a product may be classified, these Agreements provide for non-discriminatory treatment and promote broader free trade in such products. ***The FTAs also expand market access commitments in Computer and Related Services and ensure that establishment in either country is explicitly not required for the provision of services.***

many smaller and medium sized enterprises, which SIIA's research indicates are having larger proportions of their revenues derive from outside North America.[6]

From our vantage, the risks are not only regulatory compliance costs and contradictions. It is also the direct risk that, under the rubric of data protection, data security and data retention laws, governments will impose barriers to commerce on the Internet that undermine the U.S. Internet economy and our nation's jobs.

SIIA agrees that disparate approaches to commercial data privacy can create barriers to both trade and commerce, harming both consumers and companies. Further, SIIA also agrees that the U.S. Government should continue to work toward increased cooperation globally and to encourage global interoperability of laws across countries.

At minimum, the Department should be especially vigilant to the risk of data protection laws serving as trade barriers, factor this risk into its engagement with trading partners in both a multilateral and bilateral context and continue its on-going efforts to facilitate cross-border mechanisms, as well as seek appropriate common arrangements that further this objective.

For example, the Department's role in negotiating and implementing the US-EU Safe Harbor agreement stands as a hallmark of DOC leadership and expertise. For many members of SIIA, and other US enterprises with customers and operations in the European Union, the Safe Harbor agreement is an essential mechanism to foster cross-border information flows and satisfy different jurisdictional regimes. In addition, the work of the USG, in partnership with U.S. industry, has been important to provide for model contracts to satisfy EU requirements in order that personal data can flow from a Data Controller established in the EU to a Data Controller established outside the EU.[7]

Further, SIIA concurs that the development of key principles, based on the APEC Privacy Framework, is a laudable approach to achieving greater interoperability, one that protects privacy while preserving the flexibility necessary for innovation.

It is essential that the Department support efforts to further the success of the 2008 APEC Ministerial that affirmed the "Digital Prosperity Checklist" and recognized the need to "Promote the development and operation of data privacy frameworks that maximize both privacy protection and the continuity of cross-border information flows consistent with the 2004 APEC Privacy Framework."[8] SIIA encourages the USG to consider the opportunities afforded by efforts such as the Trans-Pacific Partnership to further these goals. In addition, the USG should explore meaningful engagements with non-EU trading partners on how to foster cross-border flow of personal data without the context of the EU Data Protection Directive.

---

[6] See *Software and Information: Driving the Global Knowledge Economy*, discussion beginning on pg. 31.

[7] See http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm.

[8] See note on the work of the APEC Electronic Commerce Steering Group, available at: http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.html.

As the Task Force carries out its work in the area of securing personal date, it will be essential to emphasize, based on global principles and the U.S. "Safeguards Rule" the need for on-going data security plans in a manner that promotes predictability and certainty for consumers, consumer protection authorities and businesses. This is not only good policy and practice, but also challenges other government that may seek to micromanage technical implementation of data security obligations.

SIIA summarizes the following principles based on international principles,[9] experts[10] and existing regimes, particularly the U.S. "Safeguards Rule,"[11] which are all appropriate regardless of the size of the entity.

As a fundamental matter, the companies and entities that own or license sensitive personal information should develop a written information security plan that describes their program to protect such information. The plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the information it handles.[12] Stated another way, the promotion of on-going security plans should avoid micromanaging the details of the plans, since effective security plans will be based on risk and threat analysis, and implementation details that are unique to each entity's situation, taking into account a variety of factors that overt regulation cannot foresee or be flexible enough to adapt to in a rapid manner.

As a general matter, the experience to date suggests that each plan should include the following items, tailored to each entity's risk analysis and situation:

- designate one or more employees to coordinate its information security program;[13]
- identify and assess the risks to customer information in each relevant area of the company's operation (including, in particular) four areas that are particularly

---

[9] Organization for Economic Cooperation and Development (OECD), "OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" (December 2005) ("OECD Guidelines"), found at: http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html.

[10] "Final Report of the Advisory Committee on Online Access and Security" (May 15, 2000) ("Advisory Committee Final Report"), found at: http://www.ftc.gov/acoas/papers/finalreport.htm#III.

[11] Standards for Safeguarding Customer Information Rule ("Safeguards Rule"), 16 C.F.R. Part 314, issued pursuant to Title V of the Gramm-Leach-Bliley Act ("GLB Act"), 15 U.S.C. ' 6801 *et seq*..

[12] See, e.g., "Safeguards Rule." See, also, "OECD Guidelines", p. 12 ("Systems, networks and policies need to be properly designed, implemented and co-ordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organization's systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system."); "Advisory Committee Final Report", Sec. 3.4.4. ("…adopt security procedures (including managerial procedures) that are 'appropriate under the circumstances.' 'Appropriateness' would be defined through reliance on a case-by-case adjudication to provide context-specific determinations.")

[13] "Safeguards Rule", 16 C.F.R. 314.3(a).

important to information security: employee management and training; information systems; detecting and managing system failures; and on-going evaluation of the effectiveness of the current safeguards for controlling these risks;[14]

- design and implement a safeguards program, and regularly monitor and test it;[15]
- select service providers that can maintain appropriate safeguards, making sure that contracts with such service providers require them to maintain safeguards, and oversee their handling of customer information;[16] and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.[17]

To emphasize the experience of our industry to date: These requirements are designed to be flexible, appropriate to an entity's own circumstances and updated on an on-going basis. In addition, companies must consider and address any unique risks raised by their business operations—such as the risks raised when employees access customer data from their homes or other off-site locations, or when customer data is transmitted electronically outside the company network. These principles urge that rather than promoting an overtly micromanaged legal regime, national or regional frameworks should obligate entities or companies to assess and address the risks to information in all areas of their operations and implement security plans accordingly.

National Requirements for Security Breach Notification

Without question, the myriad state and Federal regimes on privacy, including data protection, data security and data breach impose increasingly confusing and conflicting requirements, ultimately have unintended consequences for consumer harm and innovation. This is an area that merits close scrutiny by the Government, and specifically the Task Force. We therefore urge that policy recognize the key role that government agencies play in promoting more effective security practices and effectuate steps that minimize the likelihood of data breaches by public authorities:

---

[14] "Safeguards Rule", 16 C.F.R. 314.3(b). See, also, "OECD Guidelines" ("Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements.")

[15] "Safeguards Rule", 16 C.F.R. 314.3(c). See, also, "OECD Guidelines" ("Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures. New and changing threats and vulnerabilities are continuously discovered. Participants should continually review, reassess and modify all aspects of security to deal with these evolving risks.")

[16] "Safeguards Rule", 16 C.F.R. 314.3(d).

[17] "Safeguards Rule", 16 C.F.R. 314(e).

At least 46 states (plus the District of Columbia, Puerto Rico and the Virgin Islands) as well as the FTC (under the Health IT Act and through actions under its existing authority for failure to maintain or disclose security practices) and Department of Health and Human Services are implementing data breach regimes.

The following objectives, in our view, have emerged from the implementation of these regimes:

Establish a meaningful threshold for notification to affected individuals. To ensure that notification is part of a coherent approach to combating the pernicious effects of identity theft, a legal regime should require notification to consumers when the security of sensitive personal information has been breached in a manner that creates a ***significant risk*** of identity theft. This is the recommendation of consumer protection authorities such as the FTC, for example.[18]

A meaningful threshold predicated on a "significant risk" standard is essential to avoid over-notification of consumers. As then-Chairman of the FTC Deborah Majoras stated in Congressional testimony:

> "The challenge is to require notices *only* when there is a likelihood of harm to consumers. There may be security breaches that pose little or no risk of harm, such as a stolen laptop that is quickly recovered before the thief has time to boot it up. Requiring a notice in this type of situation might create unnecessary consumer concern and confusion. Moreover, if notices are required in cases where there is no significant risk to consumers, ***notices may be more common than would be useful***. As a result, ***consumers may become numb*** to them and fail to spot or act on those risks that truly are significant. In addition, ***notices can impose costs on consumers and on businesses,*** including businesses that were not responsible for the breach. For example, in response to a notice that the security of his or her information has been breached, a consumer may cancel credit cards, contact credit bureaus to place fraud alerts on his or her credit files, or obtain a new driver's license number. Each of these actions may be time-consuming for the consumer, and costly for the companies involved and ultimately for consumers generally."[19]

---

[18] In testimony before the U.S. Congress, then-Chairman Deborah Majoras of the FTC stated the view of regulators that: " … companies … notify consumers when the security of this information has been breached in a manner that creates a significant risk of identity theft. Whatever language is chosen should ensure that consumers receive notices when they are at risk of identity theft, but not require notices to consumers when they are not at risk. … the goal of any notification requirement is to enable consumers to take steps to avoid the risk of identity theft. To be effective, any such requirement must provide businesses with adequate guidance as to when notices are required." Prepared Statement of the Federal Trade Commission on Data Breaches and Identity Theft, Presented by Chairman Majoras and the Other Members of the Commission Before the Committee on Commerce, Science, and Transportation of the United States Senate (June 16, 2005), p. 7. Found at: http://www.ftc.gov/os/2005/06/050616databreaches.pdf. (Hereinafter referred to as "Majoras Testimony."

[19] Majoras Testimony at p. 10. (emphasis added)

In April 2007, the Identity Theft Task Force, co-chaired by the FTC and the Department of Justice, and comprised of 17 federal agencies with the mission of developing a comprehensive national strategy to combat identity theft, reached the same conclusion: a national standard should be established to require private sector entities to safeguard the personal data they compile and maintain and "to provide notice to consumers when a breach occurs that poses a significant risk of identity theft."[20]

The establishment of a meaningful threshold is essential as there may be direct and harmful unintended consequences that may be associated with broad notification. For example, the experiences with notification regimes to date have demonstrated that consumers have been subjected to fraud scams and "phishing" attacks when bad actors hear through the media about notifications.

The concern is based on the fact that consumers are being preyed upon by bad actors following massive notifications. In January 2006, the New York State Consumer Protection Board advised that scam artists were trying to cash in on the national paranoia over identity theft by luring victims with a phony warning that they may already be the victims of identity theft.[21] The FTC was compelled to caution U.S. veterans in 2006 "to be extra careful of scams following the recent data breach at the Department of Veterans' Affairs," noting that "[i]n the past, fraudsters have used events like this to try to scam people into divulging their personal information by e-mail and over the phone."[22]

Such scams follow a simple, but serious pattern: Users may receive emails purporting to come from their credit card company or bank, referencing recent news reports of "breache,s" asking them to enter their details and account numbers for the purposes of fraud protection or to reactivate their account. Often emails may even claim a fraud has been committed against the user's account and against the backdrop of a widely reported data breach, many users will assume that news is legitimate.[23]

Careful coordination with enforcement authorities is essential to mitigate harm to consumers in the event of a breach. Based on the practical experience that where a breach occurs it is essential to act rapidly to prevent the subsequent harmful affects, a categorical requirement such as this may be inappropriate, and potentially counterproductive.

The decision as to whether or not individual notification is required in the event of a breach must be based on an analysis of the level of risk of harm on a case-by-case basis. This is absolutely essential, due to the fact that public notification of data

---

[20] The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* ("Strategic Plan"), *available at* http.//www.idtheft.gov, p. 4.

[21] See "Phishing Fraudsters Prey on Identity Theft Fears," January 13, 2006, found at: **http://www.consumeraffairs.com/news04/2006/01/cpb_phishing.html**.

[22] "FTC Warns Veterans to Delete Unsolicited E-mails;***Scams via E-mail and Telephone Often Follow Data Breaches*,**" (June 2, 2006), found at: **http://www.ftc.gov/opa/2006/06/fyi0632.htm.**

[23] See "Will MasterCard breach breed new wave of phishing?", 21 June 2005. Found at: **http://software.silicon.com/security/0,39024655,39131331,00.htm**.

breaches is a complex issue with significant implications for organization and individuals as well as law enforcement, data protection, and consumer protection authorities.

Where a breach occurs, and there may be a significant risk of identify theft, entities experiencing the breach will need to work in a time-sensitive manner with relevant law enforcement authorities who are empowered to combat computer hacking, consumer fraud and related crimes. It is essential that these vital steps are not impeded by requirements that are not as time sensitive. Moreover, it is essential that coordination be required among government authorities.

Define carefully the kind of personally identifiable information that is covered by notification requirements. Central to an effective framework is a meaningful definition of "sensitive personal information" that is relevant to combating the pernicious effects of identity theft. It is essential that a careful circumscribed set of "sensitive personal information" be the basis for determining whether any notification occurs.[24] Two very important points:

- It should not include a breach involving elements that are widely used in commerce to facilitate transactions.

- It also makes no sense to require companies to impose additional security requirements on or notify consumers of security breaches on information that is already widely available and in the public domain.[25]

Avoid mandating specific technologies, while encouraging the adoption of good practices. SIIA would urge, as part of a coherent national framework, technology-neutral incentives for businesses to take appropriate and effective steps to safeguard sensitive data. A number of security methods and practices are available to businesses and government, including encryption, truncation, access controls, anonymization and redaction. To single out one method to secure data in legislation, such as encryption, suggests, if not an outright mandate, then a *de facto* exclusive means to avoid notification, creating a false sense of security. Singling out one methodology would not be in the overall best interests of the security marketplace, since it may reduce the development and use of diverse and innovative security tools. SIIA strongly recommends that "securing the information by a method that renders the data elements unreadable or unusable" is recognized in policy.

---

[24] In general, sensitive personal information that, if breached, should be subject to notification, should include first and last name in combination with any of the following: (A) Government issued identification number used to facilitate social welfare benefits or the equivalent; or (B) Financial account number or credit card or debit card number of such individual, combined with any required security code, access code, or password that would permit access to such individual's account.

[25] It is noted that the vast majority of U.S. states that have enacted data security breach notification laws (35 of the 39 to date) have included an exception for public record information.

Where 3rd parties manage data, and notification is required, avoid consumer confusion. In cases where a 3rd party manages "sensitive personal information" of consumers for entities that own or possess sensitive personal information, notification requirements should be constructed to avoid consumer confusion. The best way to achieve this end is to obligate the third party to notify the entity that owns or licenses the data – i.e., the entity that has the relationship with the person whose sensitive personal information may have been breached. The entity that owns or licenses the sensitive personal information should, in turn, notify the end user or consumer. Otherwise, individuals are unlikely to recognize the source of the notice and thus unlikely to act in a manner to protect themselves, which is the object of notification regimes.

Electronic Surveillance and Commercial Information Privacy

SIIA agrees that the Administration should review the Electronic Communications Privacy Act (ECPA), particularly in light of the tremendous technological advances in communications and computing technology that the world has witnessed since 1986, when the statue was passed. Given the rise of networked computing, including but not limited to cloud computing, the law needs to be updated to protect individuals from unwarranted government intrusion in the online world no less than they do in the home, even as communications and computing technology continue to advance. Currently, it runs the risk of stifling the next wave of computing where users increasingly rely on third parties to store communication information such as email, either in the cloud or otherwise.